网络安全规划交流

唐龙 2024.3.23

Presenter name

www.islide.cc

交流内容

1. 什么是IT规划
2. 信息安全规划是什么
3. 如何进行网络安全规划

什么是IT规划

什么叫做IT规划

自上而下-战略规划

规划是什么?

1、对长期

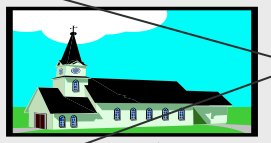
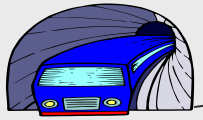
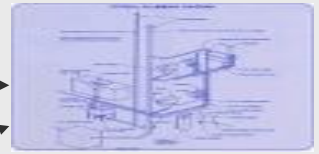
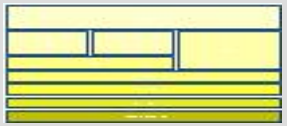
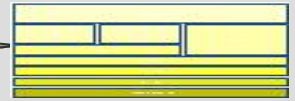
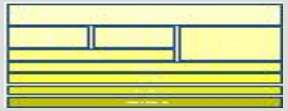
PLAN

步执行?

2、对当前的需求进行分析，给出相应的架构?

自下而上-计划

规划就是从整体到细节的分解

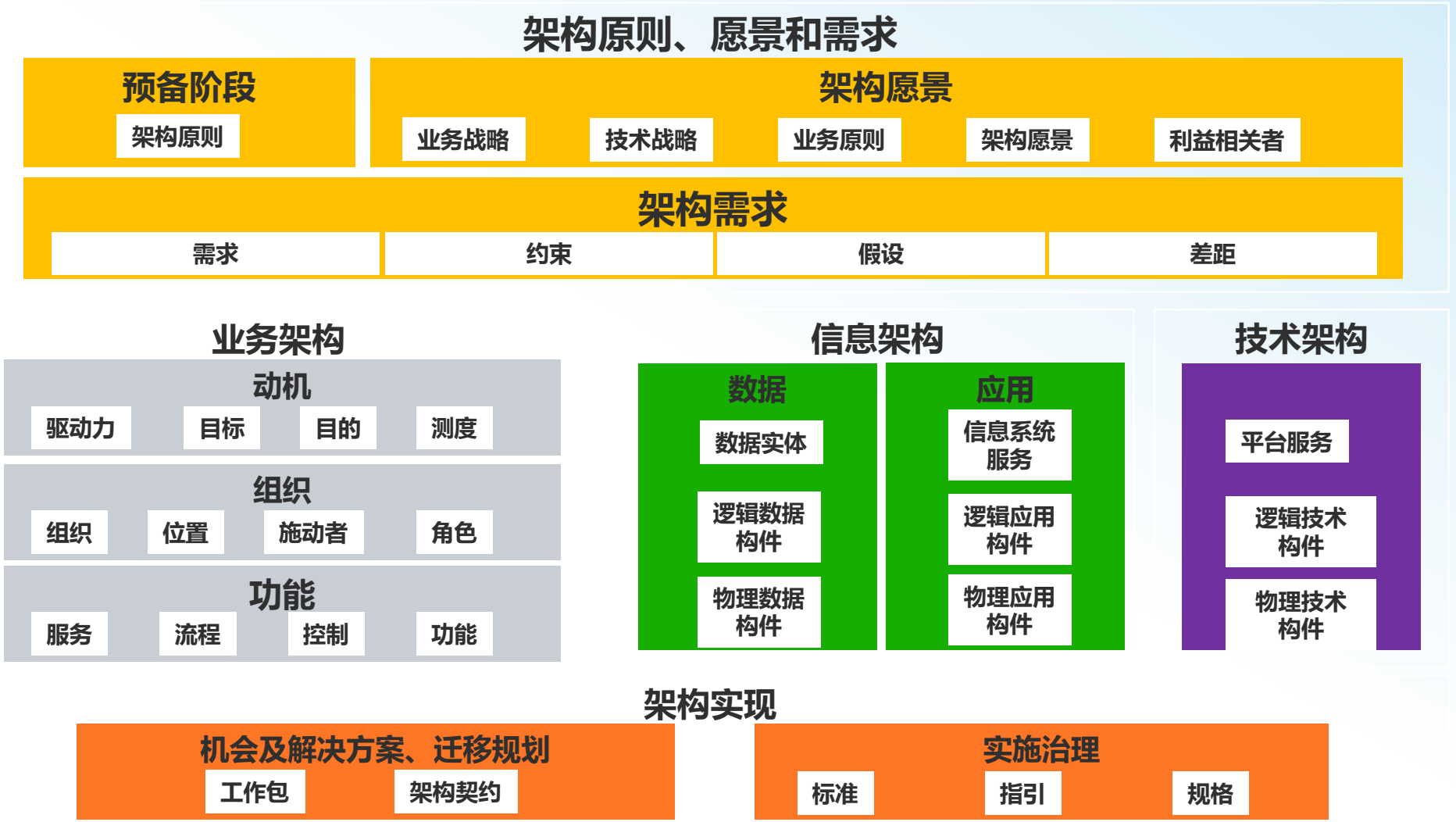
总体规划	功能区规划设计	工程局部设计
城市规划建设过程		
 城市的规划图	 教育设施  居民住宅  工业园区	 XX综合区外观设计  管道、排水、网络布线设施设计
企业的IT建设过程		
 企业架构	 财务系统  供应链系统  产品数据管理系统	 XX系统解决方案设计  XX系统方案设计

- 企业架构就像企业的“城市总体规划蓝图”，在它的指导下，各个IT系统的建设得以有序的开展

ZACHMAN-解决系统建设的问题，最原始的规划方法

	是什么	怎么做	在哪里	是谁	什么时间	为什么	
高级管理层	目录标识	过程识别	区域识别	责任认定	时间识别	动机识别	上下文范围
业务管理者	概念定义	流程定义	区域定义	责任定义	时间定义	动机定义	业务概念
架构师	实体	流向	分布	角色权限	生命周期	标准模型	系统逻辑
工程师	对象规格	流程规范	分布规范	责任规范	时间规范	动机规范	技术物理
技术员	对象配置	流程配置	分布配置	责任配置	时间配置	动机配置	工具组件
用户客户	对象实例	流程实例	地区实例	责任实例	时间实例	动机实例	操作实例
	目录集	过程流	分销网络	责任分配	时间周期	动机的意图	

TOGAF是目前的IT规划主流思想



信息安全规划是什么

为什么信息安全需要规划

信息安全在大部分企业的痛点：

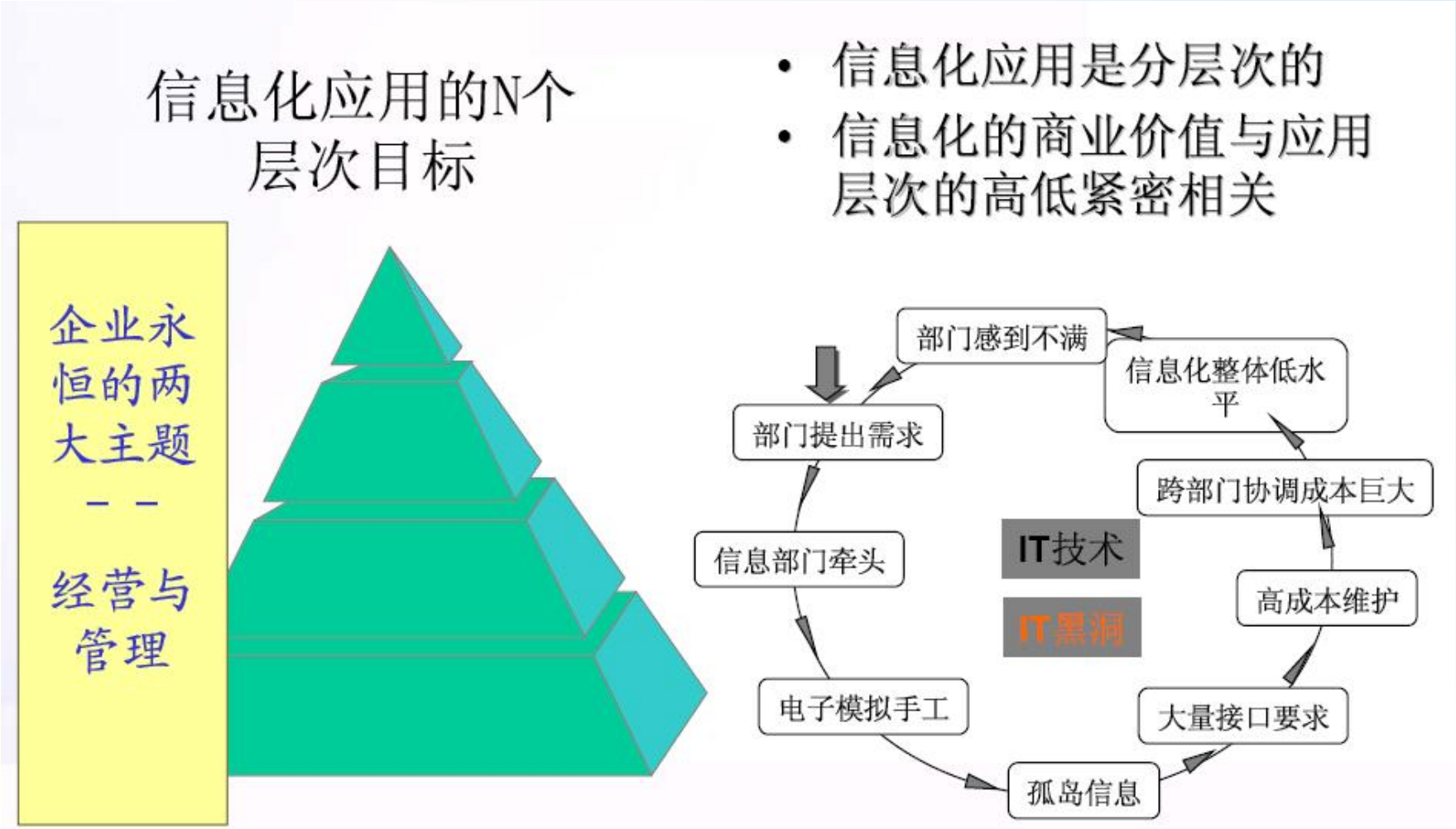
1、花钱多

2、实际没效果

3、原有的传统技术市场早就饱和，被数字化环境证明千疮百孔

4、业务压根就觉得没作用，折腾人的东西

IT以前是否也有类似的问题?

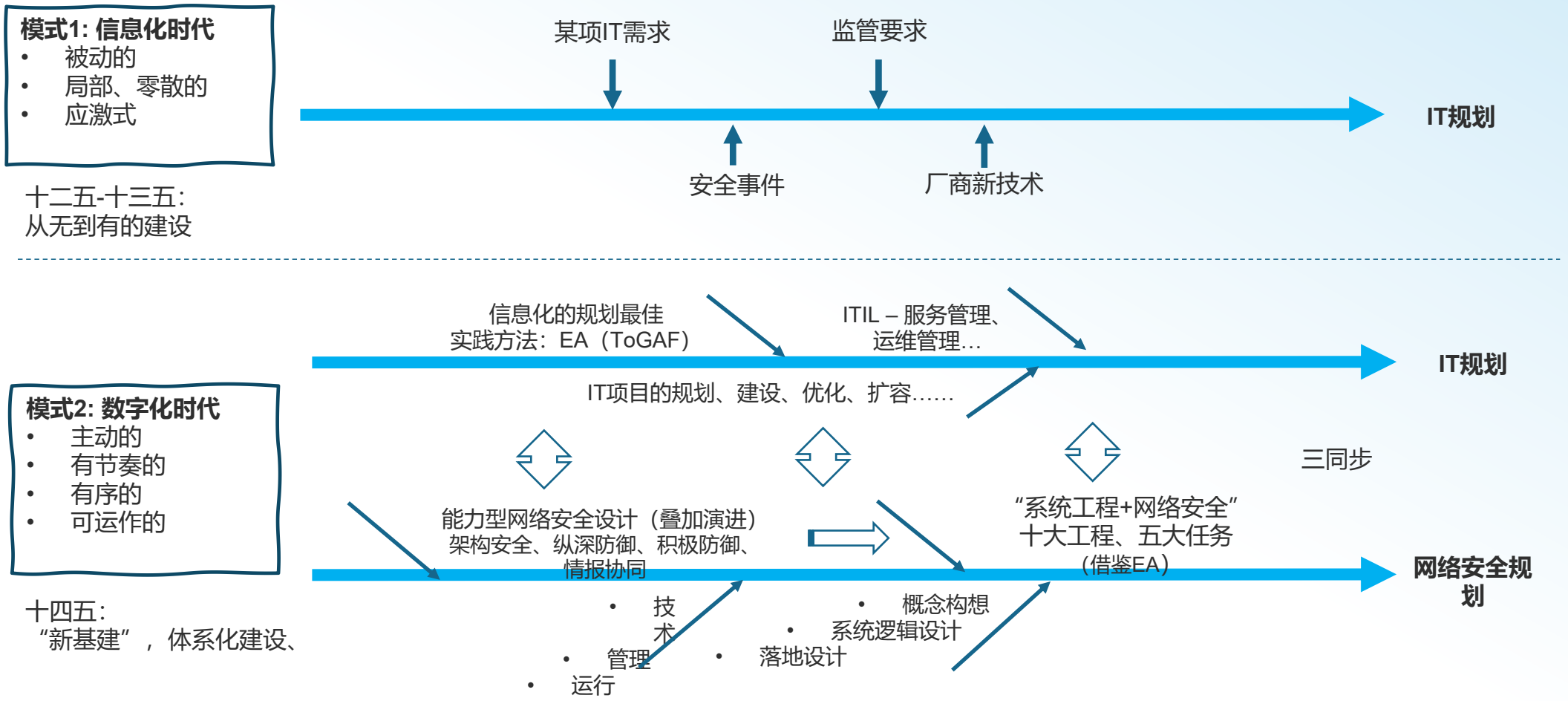


当前网络安全的痛点

- 网络安全在理论层面没有与**EA、ITIL**同等层次的、以**系统工程思想**引导的规划与建设实践，导致形成了以**“局部整改”**为主的安全建设模式，致使网络安全**体系化不足、碎片化严重、协同能力差、可弹性恢复能力严重缺失**。

- 这种局部整改模式，造成惯性的认知，安全就是买盒子、就是应对检查。**本质上是安全理念缺乏对网络安全系统性、动态性的理解，安全建设模式被固化了，看不清网络安全体系的全景框架，**随着数字化业务运营对安全要求提高，所有人对保障数字化时代的网络安全缺乏信心。

业务数字化转型带来的是安全体系化的转变



安全体系化的建设，能够体系化看出所有的痛点

普遍性问题

与业务融合度不高：安全未能真正成为业务的一部分。安全与信息化的距离太远，与业务更远，对业务的价值不明显。

缺乏方法论指导：未能像IT一样采用类似EA的系统工程方法论指导，安全建设不成体系，形成了零敲碎打、局部整改模式。

缺资源：资源保障长期不充足。

1. 因为规划里面没定义出来关键任务、技术路线，不知道在那些地方投入。
2. 认为安全已经做得到位了，不需要再持续投入。

缺人：因为大量工作没有显性出来，大量必要的工作缺相应的负责人。

缺运行：运行不闭环。大量隐性工作，没有纳入运行；应急能力差；部门协同障碍。

人防与技防结合不足：非安全岗人员安全意识不足，觉得安全和自己无关。技术上缺乏足够的技术手段去控制，导致制度无法落实。

缺协同：用了很多技术，整合不起来，碎片化、能力割裂，发挥不了作用。

缺应急：安全资源、能力就绪度低

缺条令：安全运行可持续性差。大量隐形工作未显化，不知道干什么事情，没有人干。

缺技术：广度不足、深度不深，落地不到位。

缺基础：安全体系基础设施不完备，IT资产管理混乱，基础较弱，不能完全知道要保护哪些IT资产?

缺深度：与信息化各层次结合程度不高，不深入，两张皮

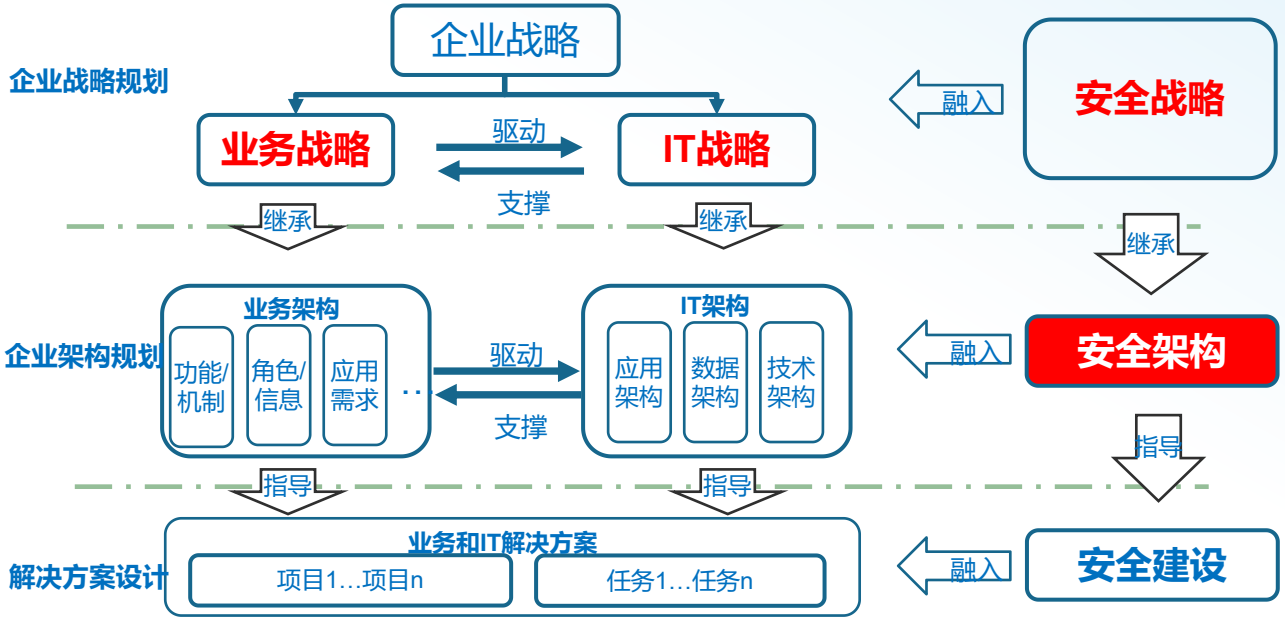
缺广度：安全对信息化环境的覆盖面不全，盲点导致整个安全体系失效。（木桶效应）

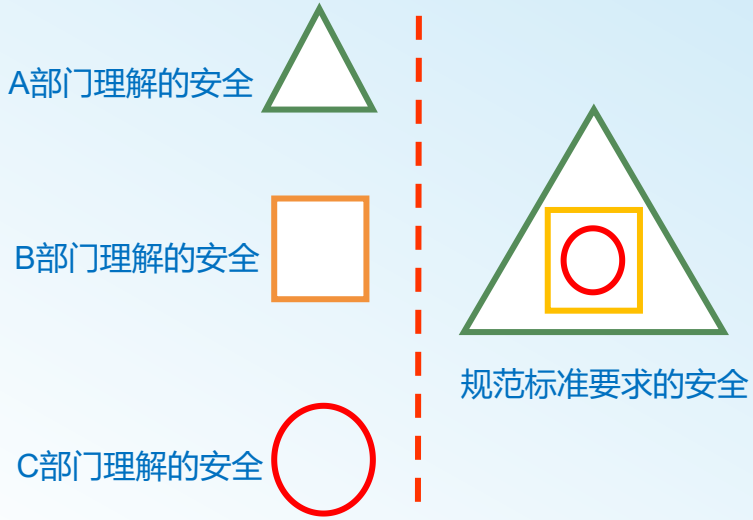
缺乏全景框架：看不清、看不全缺乏框架指导。

安全需要有IT规划类似的方法-SABSA

	资产（什么）	动机（为什么）	过程（如何）	人（谁）	地点（何地）	时间（何时）
背景层	业务	业务风险模型	业务过程模型	业务组织和关系	业务地理布局	业务时间依赖性
概念层	业务属性配置文件	控制目标	安全战略和架构分层	安全实体模型和信任框架	安全域模型	安全有效期和截止时间
逻辑层	业务信息模型	安全策略	安全服务	实体概要和特权配置文件	安全域定义和关系	安全过程循环
物理层	业务数据模型	安全规则、实践和规程	安全机制	用户、应用程序和用户接口	平台和网络基础设施	控制结构执行
组件层	数据结构细节	安全标准	安全产品和工具	标识、功能、行为和访问控制列表（ACL）	过程、节点、地址和协议	安全步骤计时和顺序
运营层	业务连续性保障	运营风险管理	安全服务管理和支持	应用程序和用户管理与支持	站点、网络和平台的安全	安全运营日程表

安全需要有IT规划类似的方法- TOGAF





融合

指引

EA	业务架构	数据架构	应用架构	技术架构	安全架构
第1层	业务域	数据域	应用域	技术域	安全域
第2层	业务分类	数据主题	应用	技术平台	安全要求
第3层	业务事项	概念实体	一级 应用模块	一级 技术模块	安全措施
第4层	业务流程	逻辑实体	二级 应用模块	二级 技术模块	安全能力
第5层	流程环节	物理实体	应用功能 应用组件	技术功能 技术组件	安全平台 安全组件

复杂系统：运行作为复杂系统，要考虑设定/尊重/引导不同的个体目的。不同的目的，可以有多种较为标准化的工具和方法联合实现，然后这些个体目的共同连接在一起实现复杂系统的目的。

如何进行信息安全规划

安全规划方法论

规划项目实施活动

现状分析

搜集 汇总 研讨 分析 安全规划需求

- 业务现状调研
- 信息化现状调研
- 安全能力现状调研
- 差距及挑战分析

规划安全战略

- 信息化战略分析
- 网络安全战略目标制定
- 网络安全能力体系制定

目标安全体系展望

管理

保障业务

技术 运行

项目规划与路线图设计

- 急迫性
- 重要性
- 可行性

可研与立项

- 数据安全
- 态势感知
- 云安全
- ……

知识传递

实施内容&工具

调研访谈模板（工具）

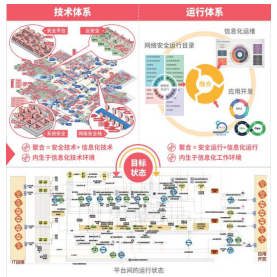
- 等级保护 ISO27001 NIST CSF
- 最佳实践（对标）
- 风险识别（威胁分析）
- 奇安信咨询规划经验

网络安全能力体系

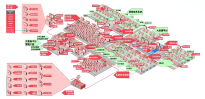
网络安全能力评价模型（工具）

项目库（工具）

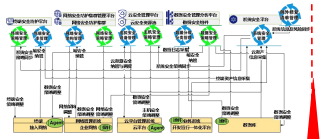
网络安全体系参考架构（工具）



网络安全防御全景模型（工具）



网络安全协同联动模型（工具）



项目规划与路线图设计（工具）

投资概算模板（工具）

现状分析报告

安全体系规划设计报告

项目规划与演进路线报告

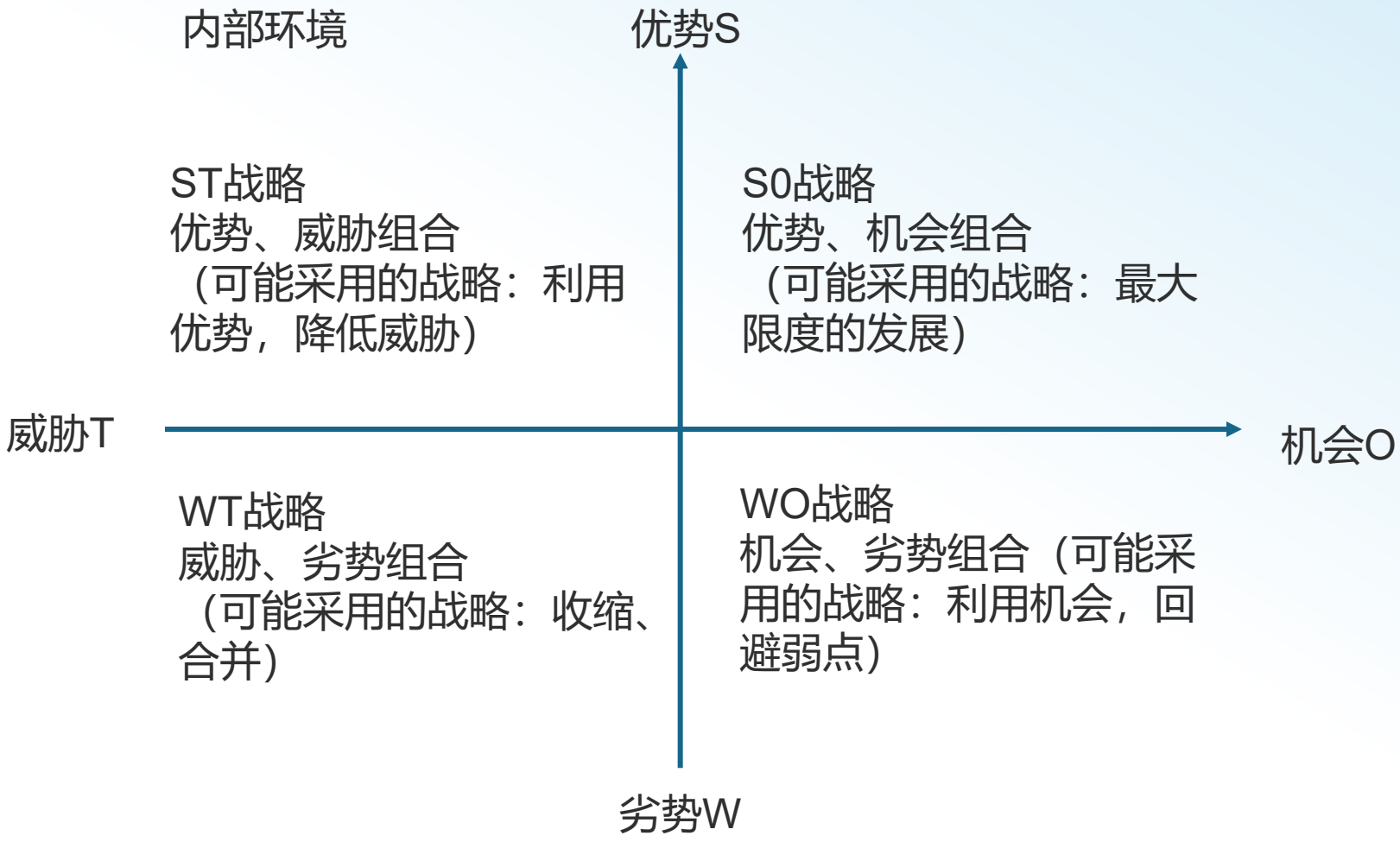
重点项目可研报告

现状分析-安全成熟度评估

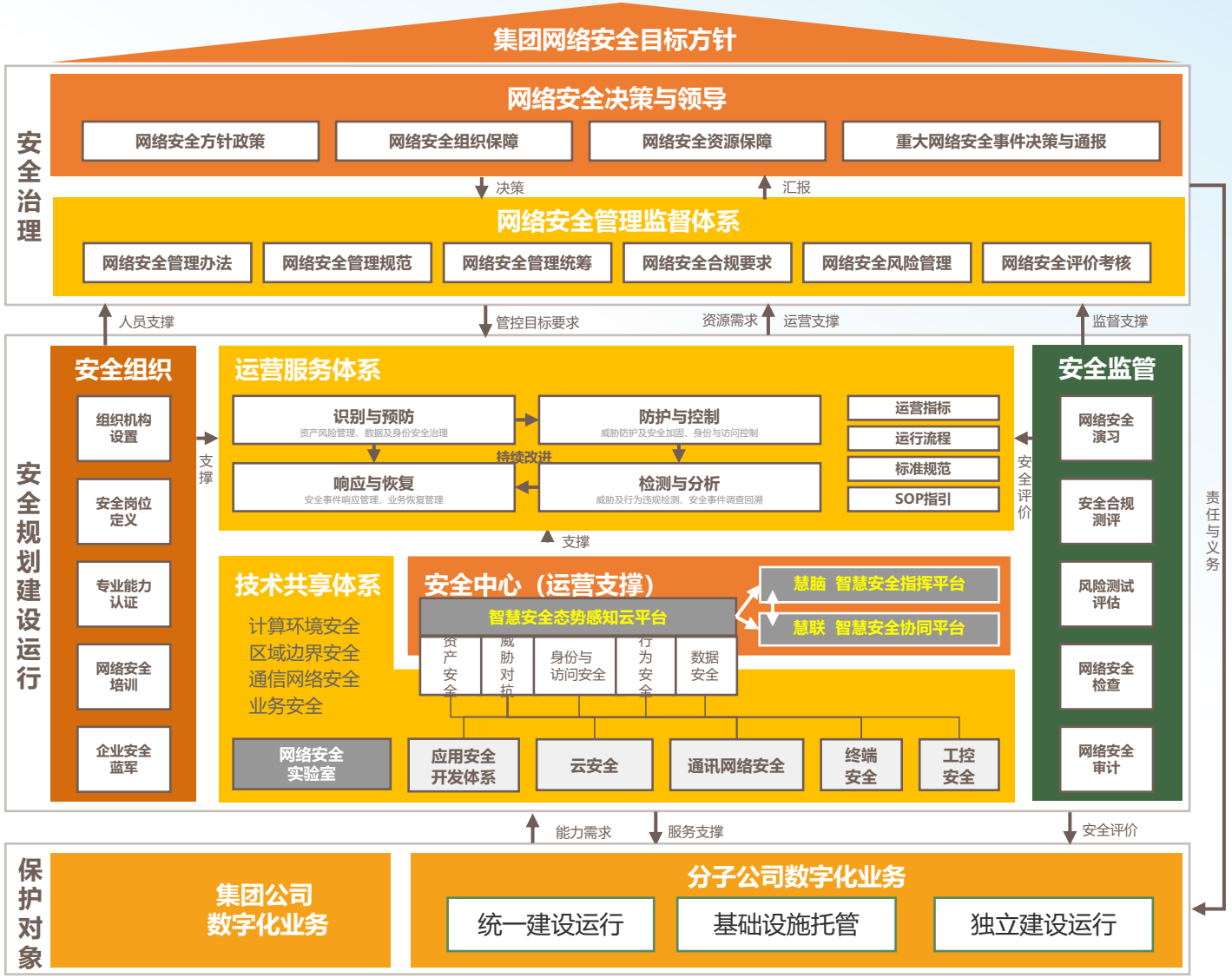
	战略与组织	机制与流程	技术与服务	人才与技能	合规建设
等级五	在等级四的基础上增加：通过自动化的平台进行固化，持续性进行优化。	在等级四的基础上增加：通过自动化平台固化机制和流程，依据执行成效和过程数据持续改进。	在等级四的基础上增加：通过数据驱动的威胁分析、智能决策和编排调度，动态的调整安全防护能力和安全策略，并据此开展日常化、建制化、规程化和可持续的	在等级四的基础上增加：具有充足的人才储备。能够有效推动机构和行业、生态间的长效沟通，配合国家、行业要求增加技术研究储备。	在等级四的基础上增加：建立了重大法律风险预警和应对机制，定期审定优化。
等级四	在等级三的基础上增加：网络安全工作已成为机构文化的重要组成部分，制定并维护了与国家要求、行业要求、业务发展相匹配的网络安全战略、框架、策略。	在等级三的基础上增加：通过完善的监督审计机制形成闭环，对流程中的各项工作形成操作指南，并配套以标准化的工具支撑流程推进，能够量化评价流程的执行效	在等级三的基础上增加：建立了集约化的安全基础设施、安全控制手段和攻防对抗能力，可聚合多源威胁情报对接安全资源，并在统一的平台上开展了全面的网络	在等级三的基础上增加：建立了网络安全人才框架能力模型，根据岗位职责确定各个岗位能力要求，制定了培训计划，对网络安全岗位和人员进行全生命周期的安	在等级三的基础上增加：通过平台对合规情况进行管理。建立了重大法律风险预警和应对机制。
等级三	管理层较为重视网络安全相关的工作，设置了网络安全工作的组织架构、按照计划分配资源用以支撑网络安全工作的开展。通过完善的制度、文件固化安全要求和安全策略。将安全工作成效纳	识别并建立了部分网络安全工作的机制、流程，通过监督审计机制形成闭环，对不同部门的权责边界进行了划分，各部门可以形成初步的配合，通过制度、文件固化流程，但没有操作指南。	建立了体系化的安全基础设施、安全控制手段和攻防对抗能力，能够纳管大部分信息化资产，建立了基础的防护策略，可收集威胁情报对接安全资源，开展了部分网络安全运行工作，能够主动	设计了网络安全团队，确定了各个岗位能力要求，制定了培训计划，对网络安全人员的入岗、离岗进行了有效的控制。网络安全人才占信息化人才的比例合理。能够推动机构和生态间的沟通。	全面识别属地法律、法规的要求，按要求开展安全防护工作，定期评估法律法规在改善网络安全实践方面的有效性，制定改进计划。建立了重大法律风险预警和应对机制。
等级二	管理层意识到了网络安全工作的重要性，设置了粗略的组织架构，建立了少数的管理制度，在事件驱动下进行资源的分配和网络安全工作的开展。	仅建立了少数关键的流程，确定了干系人，但流程不规范、协同工作尚存在沟通障碍。	面向主要的信息化对象，建设了较为完善的安全控制手段，开展了基础的安全设备运维工作，只能被动式的响应安全事件。	确定了网络安全各个岗位的能力要求，制定了培训计划，对网络安全人员的入岗、离岗进行了基本的控制。	识别属地法律、法规的要求，按要求开展安全防护工作。

安全战略方向-SWOT分析

安全战略方向-SWOT分析



所以，我们说的网络安全全局是什么？我们哪里缺了？

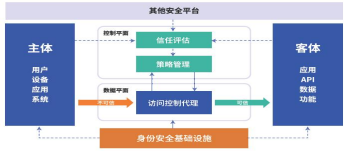


安全的管理领域

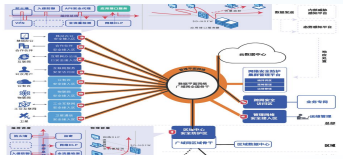
识别	保护			检测	响应	恢复
5.1信息安全策略	5.3职责分离	6.4 违规处理过程	8.7 恶意软件的控制	5.7 威助情报	5.5 与职机构的联系	5.5 与职能机构的联系
5.2信息安全角色和责任	5.5与职能机构的联系	6.5 任用的终止和变重	3.8 技术脆弱性的管理	5.25信息安全事态的评估和决策		
5.4 管理责任	5.6与特定相关方的联系	6.6 保密或不披露协议	8.9 配置管理	5.28 证据的收集	5.6 与特定相关方的联系	
5.7威胁情报	5.8项目管理中的信息安全	6.7 远程工作	8.10 信息删除	6.8 报告信息安全事态		
5.8项目管理中的信息安全	5.10可接受的信息和相关资产的使用	7.1 物理安全边界	8.11 数据屏蔽	7.4 物理安全监控	5.24信息安全事件管理责任和准备	5.6 与特定相关方的联系
5.9信息及其他相关资产清单	5.11 资产的归还	7.2 物理入口控制	8.12 防止数据泄	7.11 支持性设施		
5.12信息分级	5.13 信息的标识	7.3 办公室、房同和设施的安全保护	8.14 信息处设施的冗余度	8.6 容量管理	5.25信息安全事态的评估和决	
5.19供应商关系中的信息安全	5.14 信息传输	7,4 物理安全监控	8.17 时钟同步			
5.20供应商协议中的信息安全	5.15 访间控制	7.5防范物理和环境威胁	8.18 特权实用程序的使用	8.7 恶意软件的控制	5.26 信息安全事件的响应	5.24 信息安全事件管理责任和准备
5.21管理ICT供应链中的信息安全	5.16 身份管理	7.6 在安全区域工作	8,19在业务系统上安装软件			
5.22供应商服务的监测、审查和变更管理	5.17 认证信息	7.7 清理面和屏幕策略	8.20 网络控制	8.12 防止数据泄漏	5.28 证据的收集	
5.27从信息安全事件中学习	5.18 访问权	7.8 设备安置和保护	8.21 网络服务的安全			
5.30识别法律法规、监管和合同要求	5.23 使用云服务的信息安全	7.9 场所外资产的安全	8.22 网站过滤	8.15 日志管理	5.29 中断期间的信息安全	5.26 信息安全事件的响应
5.32知识产权	5.27 从信息安全事件中学习	7.10 存储介质	8.23 网络中的隔离			
5.33记录的保护	5.29 中断期间的信息安全	7.11 支持性设施	8.24 使用密码学	8.16 监测活动	5.30 关于业务连续性的ICT准备	
5.34 PII的隐私和保护	5.33 记录的保护	7.12 布线安全	8.25安全的开发生命周期			
5.35信息安全的独立审查	5.34 PII的隐私和保护	7.13 维护	8.26 应用程序的安全需求	8.17 时钟同步	6.4 违规处理过程	5.37 文件化的操作规程
5.36遵守信息安全的策略和标准	5.35 信息安全的独立审查	7.14 设备的安全处置或再利用	8.27 安全统架构和工程原则			
8.6容量管理	5.36 遵守信息安全的策略和标准	8.1 用户终端设备	8.28 安全编码	8.20 网络控制		
	5.37 文件化的操作规程	8.2 特权访问权	8.30外包开发			
8.8技术脆性的管理	6.1 审查	8.3 信息访问限制	8.31开发、测试和运行环境的隔离	8.29 开发和验收中的安全测试	8.16 活动监视	8.13 息备份
	6.2 任用条款和条件	8.4 对源代码的访间	8.32 变更管理			
8.30外包开发	6.3 信息安全意识、教育和培训	8.5 认证安全 8.6容量管理	8.33 测试信息的保护 8.34 信息系统审计控制	8.30 外包开发		

安全的技术和运营领域

新一代
身份安全

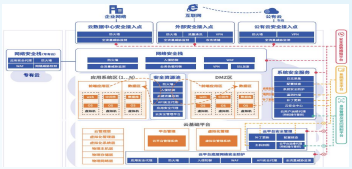


重构企业级网络
纵深防御

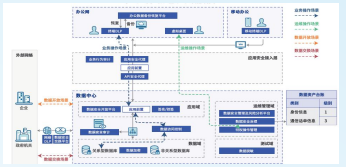


数字化终端及接
入环境安全

面向云的数据
中心安全防护

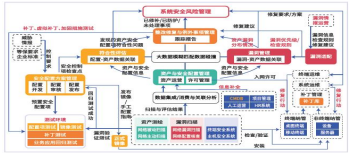


面向大数据应用
的数据安全防护



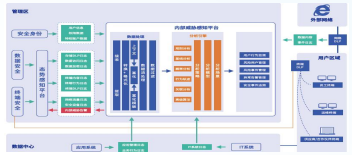
面向实战化的全
局态势感知体系

面向资产/漏洞/
配置/补丁的
系统安全



工业生产网
安全防护

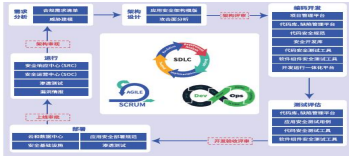
内部威胁
防控体系



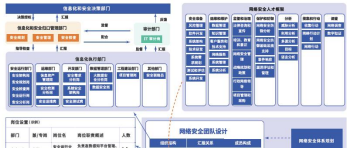
密码专项

实战化安全运行
能力建设

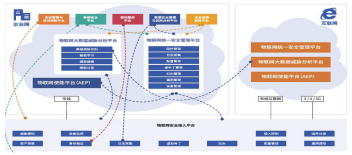
应用安全
能力支撑



安全人员
能力支撑



物联网安全
能力支撑



业务安全
能力支撑

设计能力差异的时候考虑的十个问题

1、不同级别的人的需求？业务痛点是什么？风险在哪里？有什么不合规的地方？

2、公司能拿多少钱做事？

3、公司的资产有多宝贵，风险有多高？

4、公司领导是否关注安全？

5、当前公司有多依靠IT？

6、公司的数字化水平有多高？

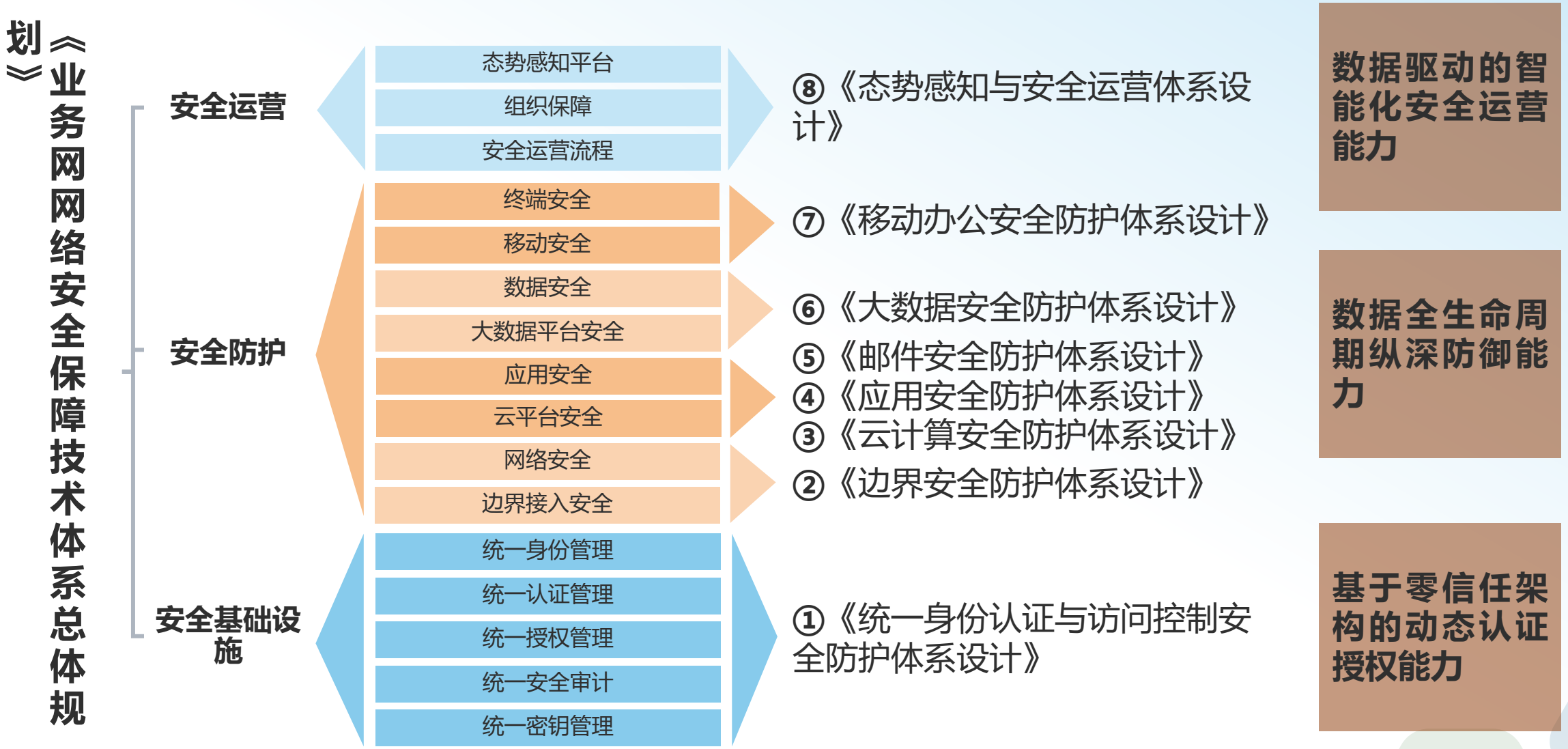
7、做的事情能够给公司带来什么价值？是刚需还是增效？

8、有没有重复投资？

9、是不是业务够用？

10、做决定之前是否和业务进行通气和同步？

最后形成了各种项目

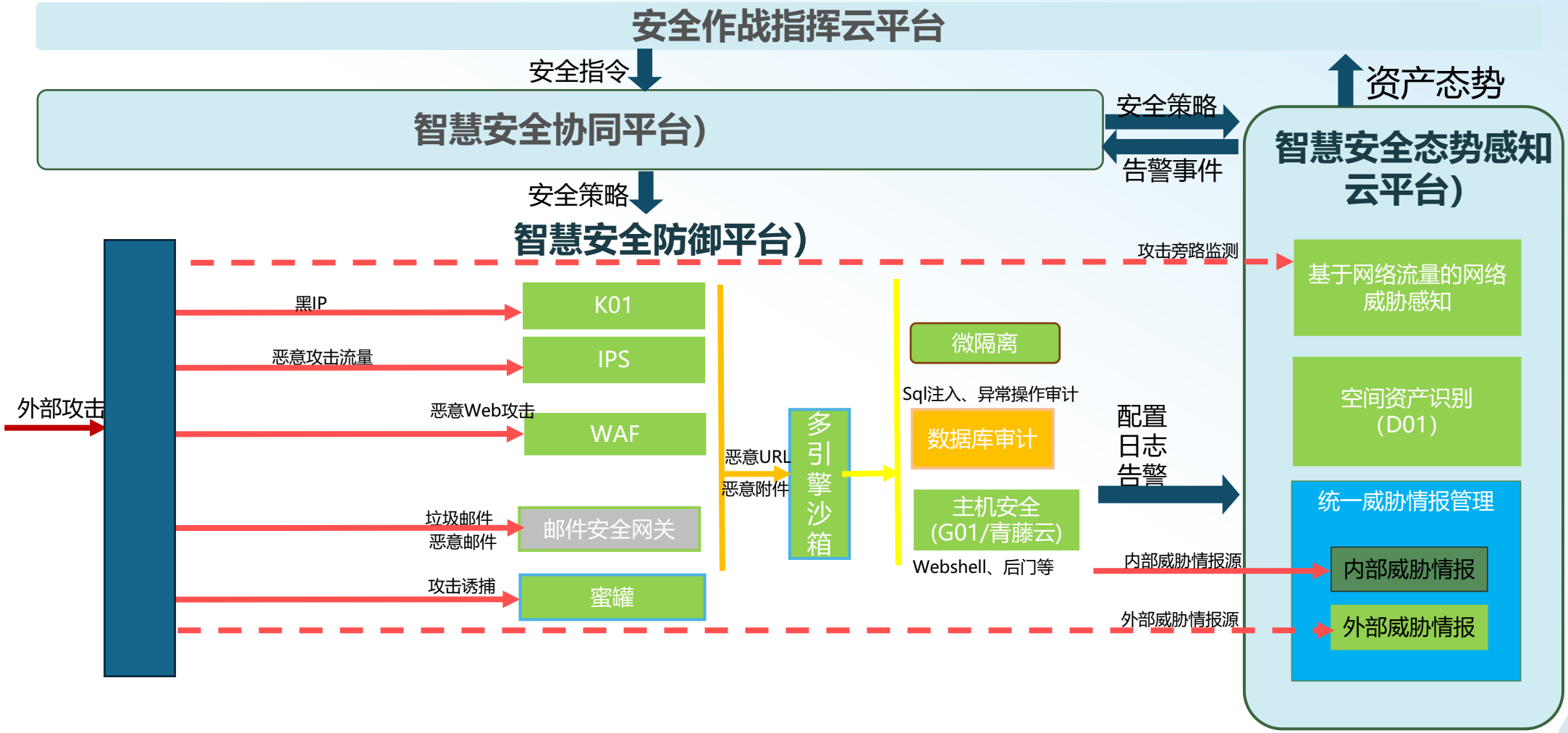

《业务网网络安全保障技术体系总体规划》
安全运营
安全防护
安全基础设施
态势感知平台
组织保障
安全运营流程
终端安全
移动安全
数据安全
大数据平台安全
应用安全
云平台安全
网络安全
边界接入安全
统一身份管理
统一认证管理
统一授权管理
统一安全审计
统一密钥管理
⑧《态势感知与安全运营体系设计》
⑦《移动办公安全防护体系设计》
⑥《大数据安全防护体系设计》
⑤《邮件安全防护体系设计》
④《应用安全防护体系设计》
③《云计算安全防护体系设计》
②《边界安全防护体系设计》
①《统一身份认证与访问控制安全防护体系设计》
数据驱动的智能化安全运营能力
数据全生命周期纵深防御能力
基于零信任架构的动态认证授权能力

最后，形成项目群和预算，第一级的规划就完成

序号	安全建设任务	2020年				2021年				2022年			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	安全防护工具建设(技术)												
2	统一身份认证及授权管理体系建设(技术)												
3	集团层面安全组织建设(管理)												
4	信息科技公司安全组织建设(管理)												
5	安全态势感知平台建设(运行)												
6	PC终端安全管控平台建设(技术)												
7	广域网边界安全防护建设(技术)												
8	数据安全管控平台建设(技术)												
9	资产安全管理平台建设(技术)												
10	业务安全审计系统建设(技术)												
11	安全要求落地平台建设(运行)												
12	安全运营服务(运行)												
13	等级保护测评服务(监督)												
14	寄递类业务安全加固(技术)												
15	应用安全测试工具建设(技术)												
16	安全管理制度建设(管理)												
17	数据安全治理服务(技术)												
18	漏洞检测工具建设(技术)												
19	安全运营管理建设(运行)												
20	软件开发安全咨询服务(技术)												
21	安全培训服务(管理)												

序号	安全建设任务	2020年				2021年				2022年			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
22	安全绩效考核建设(监督)												
23	等级保护工作管理建设(监督)												
24	云平台安全建设(技术)												
25	在线类业务安全加固(技术)												
26	数据脱敏服务系统建设(技术)												
27	基础密码服务平台建设(技术)												
28	应用架构安全加固(技术)												
29	安全合规审计建设(监督)												
30	IT外包安全风险管理建设(监督)												
31	移动生产终端采购(技术)												
32	移动生产终端安全加固(技术)												
33	防火墙策略管理平台建设(技术)												
34	非云主机安全防护建设（技术）												
35	工控-信息网侧安全加固(技术)												
36	在线业务风控平台建设(技术)												
37	大数据平台安全加固建设(技术)												
38	数据安全能力成熟度测评(技术)												
39	工控网络安全测评服务(技术)												
40	工控网络安全加固(技术)												
41	网点互联网化接入改造建设(技术)												
42	IPv6推广建设(技术)												
43	广域网SDN改造建设(技术)												

后续还需要继续落地，设计各类实施方案和细节



Thank you

Presenter name

www.islide.cc